



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/705,947	11/13/2003	Bak-Gu Lee	Q77842	6726

23373 7590 02/13/2007  
SUGHRUE MION, PLLC  
2100 PENNSYLVANIA AVENUE, N.W.  
SUITE 800  
WASHINGTON, DC 20037

EXAMINER
----------

LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
----------	--------------

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/13/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/705,947	<b>Applicant(s)</b> LEE ET AL.	
	<b>Examiner</b> Benjamin E. Lanier	<b>Art Unit</b> 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**.      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-11 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-11 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 13 November 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |  |
|--|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>6/21/05</u> . | 6) <input type="checkbox"/> Other: ____  |

## DETAILED ACTION

### *Priority*

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

### *Information Disclosure Statement*

2. The information disclosure statement (IDS) submitted on 21 June 2005 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

### *Claim Rejections - 35 USC § 101*

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 11 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 11 is directed to a computer readable medium defined in the specification as potentially being a carrier wave. Claims that recite nothing but the physical characteristics of a form of energy, such as a frequency, voltage, or the strength of a magnetic field, define energy or magnetism, per se, and as such are nonstatutory natural phenomena. O'Reilly, 56 U.S. (15 How.) at 112-14. Moreover, it does not appear that a claim reciting a signal encoded with functional descriptive material falls within any of the categories of patentable subject matter set forth in §101 (Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility Annex IV, Oct. 26, 2005, at [http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/guidelines101\\_20051026.pdf](http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/guidelines101_20051026.pdf), 1300 OG 142 (Nov. 22, 2005)).

Art Unit: 2132

5. The Supreme Court has read the term “manufacture” in accordance with its dictionary definition to mean “the production of articles for use from raw or prepared materials by giving to these materials new forms, qualities, properties, or combinations, whether by hand-labor or by machinery.” Diamond v. Chakrabarty, 447 U.S. 303, 308, 206 USPQ 193, 196-97 (1980) (quoting American Fruit Growers, Inc. v Brogdex Co., 283 U.S. 1, 11, 8 USPQ 131, 133 (1931), which in turn, quotes the Century Dictionary). Other courts have applied similar definitions. See American Disappearing Bed Co. v. Arnaelsteen, 182 F.324, 325 (9<sup>th</sup> Cir. 1910), cert. denied, 220 U.S. 622 (1911). These definitions require physical substance, which a claimed signal does not have. Congress can be presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change. Lorillard v. Pons, 434 U.S. 575, 580 (1978). Thus, Congress must be presumed to have been aware of the interpretation of manufacture in American Fruit Growers when it passed the 1952 Patent Act.

6. A manufacture is also defined as the residual class of product. 1 Chisum, §1.02[3] (citing W. Robinson, The Law of Patents for Useful Inventions 270 (1890)). A product is a tangible physical article or object, some form of matter, which a signal is not. That the other two products classes, machine and composition of matter, require physical matter. A signal, a form of energy, does not fall within either of the two definitions of manufacture. Thus, a signal does not fall within one of the four statutory classes of §101.

### ***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 6, 11 are rejected under 35 U.S.C. 102(e) as being anticipated by Kempf, U.S. Publication No. 2003/0211842. Referring to claims 1, 6, 11, Kempf discloses securing binding updates using address based keys wherein routers functioning as home agents for a mobile node, interface with mobile nodes and correspondent nodes to a core network ([0017]), which meets the limitation of a router for transmitting a packet between a mobile node and correspondent nodes. The binding updates are sent when the mobile node detects that it has moved outside its home network ([0018] & [0023]), which meets the limitation of a foreign link area. A security association is constructed between the mobile node and the home agent ([0022]) by way of cryptographic parameters generated at the home agent and transmitted to the mobile node ([0067]-[0068]), which meets the limitation of a data storage unit, which stores data for generating an authentication key generation token. Figure 1 shows that the home agent has interfaces to communicate with the mobile node and correspondent node respectively. Messages communicated between the mobile node and the home agent include a 128-bit home address assigned to the mobile node by the home agent ([0067]), which meets the limitation of a first interface, which receives and transmits a packet to a destination address stored in a header of the packet. The mobile node sends the home agent a request for the cryptographic parameters prior to the transmission of the cryptographic parameters to the mobile node by the home agent ([0067]), which meets the limitation of a packet monitoring unit, which outputs an authentication request packet requiring authentication of the mobile node if the packet transmitted from the first interface is the authentication request packet, a controller which receives a packet from the

Art Unit: 2132

packet monitoring unit, generates an authentication key generation token with reference to the data for generating an authentication key generation token stored in the data storage unit, outputs the authentication key generation token to the first interface, the first interface receives and transmits the authentication key generation token to the mobile node.

***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson, Mobility Support in IPv6 (29 October 2002), in view of Roe, Authentication of Mobile IPv6 Binding Updates and Acknowledgements. Referring to claim 1, Johnson discloses that when a mobile node is away from its home network, it registers a primary care-of address with a router functioning as a home agent (page 7). The home agent tunnels packets from the mobile node to correspondent nodes (page 7), which meets the limitation of a router for transmitting a packet between a mobile node in a foreign link area and correspondent nodes. Binding updates are

authenticated using binding management keys (page 12, 5.2). The correspondent node stores a secret key, nonces, and home or care-of addresses that are used to generate home and care-of tokens respectively (page 14, 5.2.3), which meets the limitation of a data storage unit, which stores data for generating an authentication key generation token, a controller generates an authentication key generation token with reference to the data for generating an authentication key generation token stored in the data storage unit. The mobile node transmits home and care-of test init messages to the correspondent node with the destination address in the message set as the correspondent node (pages 14-15, 5.2.5). The correspondent nodes replies to the mobile node with home and care-of test messages with the home address as the destination address (pages 15-17, 5.2.5), which meets the limitation of a first interface, which receives and transmits a packet to a destination address stored in a header of the packet, a packet monitoring unit which outputs an authentication request packet requiring authentication of the mobile node of the packet transmitted from the first interface is the authentication request packet, receiving a packet from the packet monitoring unit. When the correspondent node receives the home and care-of test init messages, it generates a home and care-of keygen token (pages 16-17, 5.2.5), which meets the limitation of generating an authentication key generation token stored in the data storage unit. The home and care-of test message include the home and care-of keygen tokens (page 16-17, 5.2.5), which meets the limitation of outputs the authentication key generation token to the first interface, wherein the first interface receives and transmits the authentication key generation token to the mobile node. The correspondent nodes creates the binding management key (page 18, 5.2.5), which meets the limitation of generating an authentication key using the authentication key generation token, storing the authentication key generation token and the

Art Unit: 2132

authentication key in the data storage unit. Johnson discloses that the key token generation is performed by the correspondent nodes, however, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform the cryptographic functionality of the correspondent nodes in the home agent/router because of the limited computational power the correspondent nodes would have being a wireless mobile device as taught in Roe (Page 11-12, 3.2 Optimization).

Referring to claim 2, Johnson discloses that the mobile node transmits a binding update to the correspondent node that includes a hash of the binding management key and mobility data (page 18-20, 5.2.6 & page 39, 6.2.6), which meets the limitation of if the packet received from the first interface is a binding update packet encoded using the authentication key generated by the mobile node according to the authentication key generation token, the packet monitoring unit outputs the binding update packet to the controller. The binding update contains the care-of address (page 39), which meets the limitation of the controller extracts binding information, including a foreign address of the mobile node provided in a foreign link area. The home address is also contained in the binding update (page 40), which meets the limitation of a home address of the mobile node. The binding update is verified using the binding management before the binding information will be stored in the binding cache (page 70-72), which meets the limitation of the binding update packet using the authentication key stored in the data storage unit, and stores the extracted binding information in the data storage unit. Johnson discloses that the key token generation is performed by the correspondent nodes, however, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform the cryptographic functionality of the correspondent nodes in the home agent/router because of the limited



Art Unit: 2132

computational power the correspondent nodes would have being a wireless mobile device as taught in Roe (Page 11-12, 3.2 Optimization).

Referring to claim 3, Johnson discloses that the traffic from the mobile node to the correspondent node goes through a reverse tunnel by received tunneled traffic from the mobile node at the home agent (page 84, 10.4.3). The tunnel entry point is the primary care-of address as registered with the home agent and the tunnel exit point is the home agent (page 84, 10.4.3). When the home agent decapsulates a tunneled packet from the mobile node, the home agent must verify that the source address in the tunnel IP header is the mobile node's primary care-of address (page 84, 10.4.3), which meets the limitation of a packet converter, which receives a packet output from the packet monitoring unit, and converts a source address of the packet from the foreign address of the mobile node to the home address of the mobile node and outputs the converted address, according to a control given by the controller, and a second interface, which receives the packet output from the packet converter, and transmits the packet to a corresponding node, according to an address of the correspondent node stored in the header of the packet, wherein the packet monitoring unit searches for the header of the packet received from the first interface, extracts and outputs binding information included in the packet header to the controller, and outputs the packet to the packet converter, the controller controls the packet converter, so that the packet converter converts the source address of the packet into the home address of the mobile node and outputs the converted address, if the binding information exists in the data storage unit.

Referring to claim 4, Johnson discloses that reverse tunneled packets may be discarded unless accompanied by a valid header, depending on the security policies used by the home agent

(page 84, 10.4.3), which meets the limitation of the controller controls the packet converter, so that the packet converter passes the packet without converting the source address included in the packet, if the binding information does not exist in the data storage unit.

Referring to claim 5, Johnson discloses that when the mobile node is away from home, the home agent intercepts any packets on the home link addressed to the mobile node's home address and forwards each packet to the mobile node by setting the source address in an encapsulated packet to the home agent's own IP address, and sets the destination address in the encapsulated packet to the mobile node's primary care-of address (page 83, 10.4.2), which meets the limitation of the packet monitoring unit outputs the destination address stored in the header of the packet received through the second interface, to the controller, and outputs a packet received from the packet converter, the controller controls the packet converter, so that the packet converter converts the destination address of the packet into a foreign address of the mobile node, if the destination address is the home address of the mobile node and the home address is bound with the foreign address of the mobile node, and the packet converter converts the destination address stored in the header of the packet transmitted by the correspondent node into the foreign address of the mobile node, according to a control given by the controller, and outputs the converted packet to the first interface.

Referring to claims 6, 11, Johnson discloses that when a mobile node is away from its home network, it registers a primary care-of address with a router functioning as a home agent (page 7). The home agent tunnels packets from the mobile node to correspondent nodes (page 7), which meets the limitation of a router for transmitting a packet between a mobile node in a foreign link area and correspondent nodes. Binding updates are authenticated using binding

management keys (page 12, 5.2). The correspondent node stores a secret key, nonces, and home or care-of addresses that are used to generate home and care-of tokens respectively (page 14, 5.2.3), which meets the limitation of a data storage unit, which stores data for generating an authentication key generation token. The mobile node transmits home and care-of test init messages to the correspondent node with the destination address in the message set as the correspondent node (pages 14-15, 5.2.5). The correspondent nodes replies to the mobile node with home and care-of test messages with the home address as the destination address (pages 15-17, 5.2.5), which meets the limitation of monitoring whether a packet transmitted from the mobile node is an authentication request packet requiring authentication of the mobile node. When the correspondent node receives the home and care-of test init messages, it generates a home and care-of keygen token (pages 16-17, 5.2.5), which meets the limitation of generating an authentication key generation token, with reference to pre-stored data for generating the authentication key generation token, if the packet transmitted from the mobile node is the authentication request packet. The home and care-of test message include the home and care-of keygen tokens (page 16-17, 5.2.5), which meets the limitation of transmitting the authentication key generation token to the mobile node. The correspondent nodes creates the binding management key (page 18, 5.2.5), which meets the limitation of generating an authentication key using the authentication key generation token and storing the authentication key generation token and the authentication key. Johnson discloses that the key token generation is performed by the correspondent nodes, however, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform the cryptographic functionality of the correspondent nodes in the home agent/router because of the limited computational power the correspondent

Art Unit: 2132

nodes would have being a wireless mobile device as taught in Roe (Page 11-12, 3.2 Optimization).

Referring to claim 7, Johnson discloses that the mobile node transmits a binding update to the correspondent node that includes a hash of the binding management key and mobility data (page 18-20, 5.2.6 & page 39, 6.2.6), which meets the limitation of receiving a binding update packet authenticated using the authentication key, the authentication key generated by the mobile node according to the authentication key generation token. The binding update contains the care-of address (page 39), which meets the limitation of the controller extracts binding information, including a foreign address of the mobile node provided in a foreign link area. The home address is also contained in the binding update (page 40), which meets the limitation of a home address of the mobile node. The binding update is verified using the binding management before the binding information will be stored in the binding cache (page 70-72). Johnson discloses that the key token generation is performed by the correspondent nodes, however, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform the cryptographic functionality of the correspondent nodes in the home agent/router because of the limited computational power the correspondent nodes would have being a wireless mobile device as taught in Roe (Page 11-12, 3.2 Optimization).

Referring to claim 8, Johnson discloses that the traffic from the mobile node to the correspondent node goes through a reverse tunnel by received tunneled traffic from the mobile node at the home agent (page 84, 10.4.3). The tunnel entry point is the primary care-of address as registered with the home agent and the tunnel exit point is the home agent (page 84, 10.4.3).

When the home agent decapsulates a tunneled packet from the mobile node, the home agent must

verify that the source address in the tunnel IP header is the mobile node's primary care-of address (page 84, 10.4.3), which meets the limitation receiving a packet transmitted by the mobile node, the packet including the binding information and data, checking whether the same binding information as the binding information included in the packet transmitted by the mobile node exists in the stored binding information, converting a source address of the packet from the foreign address of the mobile node to the home address of the mobile node, if the same binding information as the binding information included in the packet transmitted by the mobile node exists in the stored binding information, and transmitting the converted packet to the correspondent node.

Referring to claim 9, Johnson discloses that packets can be sent from the mobile node to a corresponding node without having a binding agreement by including the home address in an optional field of the packet along with the mobile node's care-of address (Page 95), which meets the limitation of transmitting the packet itself to the correspondent node without converting the source address thereof, if the same binding information as the binding information included in the packet transmitted by the mobile node does not exist in the stored binding information.

Referring to claim 10, Johnson discloses that when the mobile node is away from home, the home agent intercepts any packets on the home link addressed to the mobile node's home address and forwards each packet to the mobile node by setting the source address in an encapsulated packet to the home agent's own IP address, and sets the destination address in the encapsulated packet to the mobile node's primary care-of address (page 83, 10.4.2), which meets the limitation of extracting a home address of the mobile node stored as a destination address in the header of the packet transmitted from the correspondent node, searching for the stored

Art Unit: 2132

binding information and extracting a foreign address of the mobile node bound with the home address of the mobile node, converting the destination address of the header of the packet transmitted by the correspondent node into the foreign address of the mobile node, transmitting the packet transmitted by the correspondent node to the mobile node, according to the foreign address of the correspondent node.

### *Conclusion*

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Johansson, U.S. Publication No. 2002/0080752

Patil, U.S. Publication No. 2002/0142673

Perkins, U.S. Publication No. 2004/0236937

O'Shea, U.S. Publication 2002/0152380

Faccin, U.S. Patent No. 6,879,690

Faccin, U.S. Publication 2002/0120844

Satomi Okazaki, "Securing MIPv6 Binding Updates Using Address Based Keys (ABKs)"

Jari Arkko, "Securing Ipv6 Neighbor and Router Discovery"

John Zao, "A Public-key based secure mobile IP"

David B. Johnson, "Scalable support for transparent mobile host internetworking"

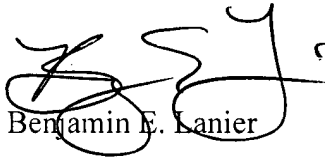
13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.

The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

Art Unit: 2132

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier